[How-To] Integrate Active Directory Authentication into OpenVPN AS

Purpose

The purpose of this how to is to show the process to add active directory authentication services to your OpenVPN access server.

Prerequisites

List of prerequisites:

- Root user or sudo user
- OpenVPN AS
- Domain Admin User
- Active Directory Domain

AD Integration Settings

Step 1: Prepare Active Directory Objects

You'll need to create a few things in Active Directory:

1. User Look Up OU:
    1. Determine the user lookup base for where it can find users, you can leave it open or at the root domain but it leaves more room for bad actors as well as slow lookups. Open the server manager and then open active directory users and computers.
    2. Find the OU that you want to use, right-click and select properties.
    3. Click the attribute editor, then find the Distinguished Name Entry. Copy this to the clipboard.
    4. Save this in your Password Manager as User Look Up OU for VPN Server AD Int.
2. Service Account to Read Users:

1. We need a service account with regular domain user permissions that can read domain users from the domain directory. Open the server manager then open active directory users and computers.
2. Find the OU where you want the service account for VPN to exist, then right-click on it and select new user.
3. In the new user entry, enter an account name as well as a domain. Then click next.
4. Set a password for the service account and repeat it. Then, remove the check for user must change password and check the boxes for password never expires as well as user cannot change password. Then click next, then finish.
5. With the user created, right-click on it and select properties.
6. Select the attribute editor and find the Distinguished Name Entry. Copy this to the clipboard.
7. Save this information along with the password in your password manager as a Service Account to Read Users for VPN.

3. Security Group to Check Users Against:
    1. If extra security is desired, you'll need a security group for VPN users that ensures not all users in your user directory have the default ability to authenticate against VPN. Only users added to the group will. Start by opening the server manager and then opening active directory users and computers.
    2. Here, find the OU where you want the security group for VPN to exist, then right-click on it and select the new group.
    3. In the new group entry, verify that security and global are selected, then click next.
    4. Now enter the name of the security group. Then click next. Then click finish.
    5. With the group created, right-click on it and select properties.
    6. Select the attribute editor and find the Distinguished Name Entry. Copy this to the clipboard.
    7. Save this information in your password manager as Security Group to Check Users Against for VPN.

This concludes our Active Directory Preparation. You will use these entries in the next steps.

Step 2: Configure AD in OpenVPN AS

Now, log in to your Web UI Admin Instance of OpenVPN AS. Browse to the Authentication and the LDAP section. Then follow these steps to configure:

1. Under the LDAP Settings section, move the slider to yes for "Enable LDAP authentication". This enabled LDAP on the OpenVPN AS.
2. Verify that the correct settings are set for SSL and case-sensitive are correct for your active directory environment, normally they will both be set to "No".
3. Verify the "Re-verify autologin user on connect" is set to "Yes". This confirms that every time users connect to the Web UI or the VPN, their credentials are verified with the active directory domain and not using cached credentials on the AS.
4. In the "LDAP Server" Section, enter the IP addresses for the primary and secondary active directory servers.

5. Also in the "LDAP Server" Section, Set "Bind anonymously" to "No" and set "Use these credentials" to "Yes". Then, use the Bind DN and Password based on the "Service Account to Read Users" Created earlier.
6. For the "Base DN for User Entries", enter the "User Look Up OU" from earlier.
7. Leave "Username Attribute" set to "sAMAccountName".
8. If you decide to use extra security, fill in the "LDAP filter" with the value from "Security Group to Check Users Against". It is important to note the instruction in red, placing "memberOf=" before the security group.
9. Click Save Settings and then scroll to the top and select Update Running Server. This enabled the LDAP connection but it does not set it to the default auth type for new user creations. This means new LDAP users who have never authenticated will not pull in when they try for the first time.
10. To make LDAP the default for new users, browse to the Authentication and then Settings tab, and select LDAP as the default. Click Save Settings, and then Update Running Server at the top of the page.
11. An additional step would be to in Authentication Settings, Move the slider temporarily to "No" for "Deny New User logins" As you'll be registering new users in the test next. When done testing it is a good idea to re-enable that.

Step 3: Test AD Auth in Browser

We have to test the AD Auth in Web UI first as that is what creates the user profile. Browse to the main public DNS for the VPN and log in with AD Creds that are in the Security Group for the VPN. If you can log in, you'll be presented with a 2FA configuration. Add it to your 2FA app on your phone and verify with the code. Once logged in, download the agent for OpenVPN Connect and the profile as well.

Step 4: Test AD Auth in VPN Client

Launch OpenVPN Connect V3 and connect on the profile you just downloaded. Enter the password for that username and then the 2FA when asked. If it connects, you have been successful.

Revision #1
Created 3 November 2024 19:57:29 by Mike Leffring
Updated 3 November 2024 19:57:57 by Mike Leffring